

REMARKS

This communication is a full and timely response to the aforementioned final Office Action dated February 21, 2008. By this communication, claims 1, 3, 4, 11, 13, 14, 19, 25 and 26 are amended. Claims 2, 12 and 24 are not amended and remain in the application. Thus, claims 1-4, 11-14, 19 and 24-26 are pending in the application. Claims 1, 11 and 19 are independent.

Reconsideration of the application and withdrawal of the rejections of the claims are respectfully requested in view of the foregoing amendments and the following remarks.

I. Rejections Under 35 U.S.C. § 103(a)

A. Claims 1, 2, 5, 11, 12, 19 and 24 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over "Unix Communication Notes: 129" (hereinafter "Notes 129") in view of Seiji (JP-5108487).

Without acquiescing to this rejection, independent claims 1, 11 and 19 have each been amended to emphasize distinctions between the claimed invention and the applied references.

Exemplary embodiments of the present invention provide a method and computer program for causing a controlling apparatus intended to control an image forming apparatus, as well as a controlling apparatus for controlling an image forming apparatus. One example configuration of the controlling apparatus is illustrated in Figure 1, in which a computer 200 is limited to controlling an image forming apparatus such as copying machine 300 (see paragraph [0023] on page 7 of the specification).

As illustrated in Figure 3, a hard disk 204 of the computer 200 includes a database 240 in which a file list 241 is stored. The file list 241 is a list of all files, such as programs, required to exist in a specific storage area of a logical drive of hard disk 204 for controlling a multifunctional peripheral (MFP) 100 that includes the computer 200 and copying machine 300 (see, e.g., paragraph [0039]). As described in paragraph [0041] on page 11, the file list 241 is set up prior to factory shipment of MFP 100 and the controlling apparatus, and is stored in the hard disk 204 of the controlling apparatus. Accordingly, the file list 241 is a prestored list of programs

and files that are authorized to be run on the controlling apparatus to control the image forming apparatus, such as the copying machine 300 illustrated in Figure 1, for example.

According to the exemplary configuration in which the controlling apparatus (e.g., computer 200) is limited to controlling an image forming apparatus, the controlling apparatus is different from a general-purpose computing device in which a user may wish to add, modify or remove programs and files at will for various purposes. On the other hand, since the function of the controlling apparatus is limited to controlling the image forming apparatus, according to the exemplary configuration illustrated in Figure 1, the preset list of programs in the file list 241 represents a limited number of programs that are authorized to be run on the controlling apparatus to control the image forming apparatus.

When a computer virus infiltrates into a computer, the virus often creates a new program and/or file. In the case of a general-purpose computing device, the number of programs and files that can be run is not limited to a preset list, because of the desire to allow users to add new programs or files and modify or delete existing programs or files. For example, general purpose computing devices are configured to allow users to add software programs containing executable and non-executable files, and add new non-executable files, such as a word processing document, for example. Therefore, conventional virus detection systems seek to compare a file against files that are known to be created by known viruses.

On the other hand, since the preset list of programs in the file list 241 represents a limited number of programs that are authorized be run on the controlling apparatus to control the image forming apparatus, the detection of a program that is not included in the file list 241 is judged to be an illegal program resulting from a computer virus infection. This judgment can be carried out because a limited number of programs that are authorized to be run on the controlling apparatus are stored in the preset list of programs.

These features of the disclosed embodiment are antithetical and disadvantageous to the functions and purpose of a general-purpose computer. In particular, limiting a general-purpose computer to a preset list of programs would defeat the purpose of permitting a user to create, add and modify files and programs

on the general-purpose computer. On the contrary, general-purpose computers are designed to allow dynamic modifications.

Claims 1, 11 and 19 broadly encompass various features of the above-described exemplary embodiment.

Claim 1 recites a computer program stored on a computer-readable recording medium and causing a controlling apparatus intended to control an image forming apparatus to execute the following procedures:

- (1) storing a preset list of programs that are authorized to be run on the controlling apparatus to control the image forming apparatus;
- (2) confirming each program running on the controlling apparatus;
- (3) judging a program, which is **not included** in a preset list of programs that are authorized be run to control the image forming apparatus among programs whose running states have been confirmed, as an illegal program resulting from a computer virus infection; and
- (4) deleting or isolating the program that is judged to be the illegal program.

Claim 11 recites a controlling apparatus for controlling an image forming apparatus. The controlling apparatus of claim 11 comprises a storage unit for storing in advance a preset list of programs that are authorized to be run for controlling the image forming apparatus. The controlling apparatus of claim 11 also comprises a processor that is configured to perform functions corresponding to procedures (2)-(3) of claim 1.

Claim 19 recites a controlling method for a controlling apparatus intended to control an image forming apparatus. The method of claim 19 comprises steps corresponding to procedures (1)-(4) of claim 1.

Accordingly, features (1)-(3) of claim 1 are common to each of independent claims 1, 11 and 19. Claims 1, 11 and 19 thus each recite that a preset list of programs that are authorized to be run on the controlling apparatus to control the image forming apparatus are stored. In addition, claims 1, 11 and 19 each recite that each program running on the controlling apparatus is confirmed, and a program, which is **not included** in a preset list of programs that are authorized to be run to control the image forming apparatus among programs whose running states have

been confirmed, is judged as an illegal program resulting from a computer virus infection.

Thus, claims 1, 11 and 19 recite that programs that are authorized to be run to control the image forming apparatus are included in a preset list of programs. This preset list therefore contains programs that are known (approved) to control the image forming apparatus. However, if a program is confirmed to be running on the controlling apparatus and that confirmed program is not included in the preset list of programs, it is judged to be an illegal program resulting from a computer virus infection.

Applicant respectfully submits that it would not have been obvious to combine Notes 129 and Seiji to arrive at the claimed inventions of claims 1, 11 and 19, for at least the following reasons. On the contrary, Applicant respectfully submits that the combination of Notes 129 and Seiji suggests a technique that is opposite in purpose and effect to the claimed invention.

Notes 129 discloses a technique for use with general-purpose computers to determine whether an illegal invader has hidden files in the general-purpose computer over time as the user of the general-purpose computer communicates with other users over computer networks (e.g., mail) or inserts computer-readable media (e.g., floppy disks, ZIP drives) into the general-purpose computer. To accomplish the objective of finding hidden files created by an illegal invader, Notes 129 discloses that a hidden file in a file system (Unix operating system) can be discovered by comparing an existing list of files present in the file system with a file list that was prepared in advance (see page 1). Notes 129 discloses that the list can be prepared periodically to check for hidden files that may be accumulated over time as the user of the general-purpose computer accesses external resources. A "diff command" is then used to determine whether the existing file list contains any files that are not present in the previously prepared file list. Accordingly, Notes 129 discloses that a hidden file in a file system can be discovered by comparing an existing list of files present in the file system with a file list that was prepared in advance.

However, in contrast to claims 1, 11 and 19, Notes 129 does not disclose or suggest that a preset list of programs are stored, where the preset list of programs

includes programs that are authorized to be run on the computer to control an image forming apparatus.

As acknowledged by the Office, Notes 129 does not disclose or suggest that a hidden file that is discovered by comparing the existing list of files with the previously stored list of files is judged to be an illegal program resulting from a computer virus infection.

In an attempt to teach this feature, the Office applied Seiji, which discloses that an illegal program results from a virus infection (see paragraph [0022]). Based on this disclosure, the Office alleged that the combined features of Notes 129 and Seiji suggest the recited features of claims 1, 11 and 29. This assertion is not supportable for the following reasons.

First, the concept of limiting the general-purpose computers of Notes 129 and Seiji to function with a preset list of programs that are authorized to be run on the general-purpose computers is antithetical and destructive to the purpose of a general-purpose computer. Notes 129 disclose a technique for detecting hidden files that may be accumulated over time as the user of the general-purpose computer modifies and adds files or programs to the general-purpose computer.

Seiji discloses a conventional virus detection process in which detected programs are compared against a list of pre-stored list of known viruses. Any obvious combination of Notes 129 and Seiji discloses an opposite configuration and technique to the recited features of claims 1, 11 and 19.

In particular, claims 1, 11 and 19 have a preset list of authorized programs stored, and if any program that is confirmed to be running is not included in the preset list of authorized programs, the program is judged to be an illegal file resulting from a computer virus infection.

On the contrary, neither Notes 129 nor Seiji disclose or suggest that a preset list of authorized programs are stored in their respective general-purpose computers. Instead, Notes 129 and Seiji suggest an opposite technique, where the users of the general-purpose computers can add or modify programs and files, which is the basic function of a general-purpose computer, and the files or programs resident on the general-purpose computer at any arbitrary point in time can be compared against a list of files that existed on the general-purpose computer in the past. Seiji discloses

that if any file or program is not found in the previous list, it is compared against a pre-stored list of known viruses to detect whether that program resulted from a computer virus.

In particular, Seiji discloses that an application program 3 can issue demands to a computer system's operating system 5, BIOS 7 or hardware 1 (e.g., printer) connected to the computer system (see paragraphs [0009]-[0011]). Seiji discloses that separate virus supervisory systems A-C respectively suitable for operation with the operation system 5, BIOS 7 and hardware 1 intercept a demand from the application program 3 and determine whether the demand is infected with a virus by comparing the demand with a pre-stored list of known viruses (see paragraphs [0016], [0017] and [0026]). The intercepting virus supervisory system A-C prohibits the demand from reaching the operation system 5, BIOS 7 and/or hardware 1 if the demand is infected with a virus that matches a virus stored in the pre-stored list (see paragraph [0016]).

Accordingly, with particular reference to paragraph [0016], Seiji discloses that illegal programs resulting from various kinds of computer virus are stored as a database which is prepared ahead of time. Therefore, Seiji discloses that a program which is included in a list of known viruses is judged to be an illegal program.

Accordingly, the combination of Notes 129 and Seiji is entirely different from features of claims 1, 11 and 19, because the combination of Notes 129 and Seiji requires *a priori* knowledge of a virus before it can be judged to be a virus.

Second, one skilled in the art would not have been motivated to modify Notes 129 and Seiji to limit a general-purpose computer to a preset list of programs that are authorized to be run to control an image forming apparatus. Such a modification defeats a primary objective of a general-purpose computer, which is to permit users to modify existing programs as desired.

Third, the combination of Notes 129 and Seiji does not result in the recited features of claims 1, 11 and 19. The combination of Notes 129 and Seiji proposed by the Office requires *a priori* knowledge of illegal files or programs to detect whether the file or program is the result of a computer virus infection.

On the contrary, claims 1, 11 and 19 judge programs that are confirmed to be running against programs that are authorized to be run. It appears that the Office

has ignored this foundational distinction between the claimed invention and the techniques of Notes 129 and Seiji for use with general-purpose computers.

In particular, claims 1, 11 and 19 confirm whether authorized programs are running on the controlling apparatus to judge whether a program is an illegal program resulting from a computer virus infection. In contrast to claims 1, 11 and 19, Notes 129 and Seiji disclose that files that did not exist at a recent comparison or files that are known to be illegal files are determined to be illegal files resulting from a computer virus infection.

One skilled in the art would not have been motivated to modify Notes 129 and Seiji to arrive at the subject matter of claims 1, 11 and 19, because to do so would defeat the principal object of a general-purpose computer, which is to permit dynamic modifications to the files and programs residing on the general-purpose computer. Implementing the features of claims 1, 11 and 19 would cripple the use of a general-purpose computer, and therefore, Applicant respectfully submits that one skilled in the art would not have been motivated to combine and modify Notes 129 and Seiji to arrive at the features of claims 1, 11 and 19.

Accordingly, for at least the foregoing reasons, Applicant respectfully submits that neither Notes 129 nor Seiji disclose or suggest:

- (1) storing a preset list of programs that are authorized to be run on the controlling apparatus to control the image forming apparatus;
- (2) confirming each program running on the controlling apparatus; and
- (3) judging a program, which is **not included** in a preset list of programs that are authorized be run to control the image forming apparatus among programs whose running states have been confirmed, as an illegal program resulting from a computer virus infection, as recited in claims 1, 11 and 19.

On page 8 of the Office Action, the Office asserted that Applicant cannot show nonobviousness by attacking references individually where the rejections are based on a combination of references.

The disclosure of the applied references has been addressed above. Applicant has not attached the references individually. On the contrary, Applicant has demonstrated that both Notes 129 and Seiji fail to disclose or suggest all the recited features of claims 1, 11 and 19.

The Office is respectfully reminded that, to establish a *prima facie* case of obviousness, the applied references must disclose or suggest all the recited features of the claims. See MPEP 2142; 706.02(j). If the applied references fail to disclose or suggest one or more of the features of a claimed invention, then the rejection is improper and must be withdrawn.

As demonstrated above, Notes 129 and Seiji each fail to disclose or suggest features (1)-(3) of claims 1, 11 and 19. Therefore, no obvious combination of Notes 129 and Seiji would result in the subject matter of claims 1, 11 and 19, since Notes 129 and Seiji, either individually or in combination, fail to disclose or suggest all the recited features of claims 1, 11 and 19.

Furthermore, Applicant respectfully submits one skilled in the art would not have reason or been motivated to modify Notes 129 and Seiji to arrive at the subject matter of claims 1, 11 and 19. The techniques disclosed in Notes 129 and Seiji are disclosed for general purpose computing devices, not for a controlling apparatus intended to control an image forming apparatus in which the programs that can be run therefor are included in a preset list of programs.

Therefore, for at least the foregoing reasons, Applicant respectfully submits that claims 1, 11 and 19, as well as claims 2-4 and 24-26 which depend therefrom, are patentable over Notes 129 and Shoji.

B. Claims 3, 4, 8, 9, 13, 14, 17 and 18 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Notes 129 in view of Seiji and further in view of Yamamoto (U.S. Patent No. 5,881,151). This rejection is believed to be moot with respect to claims 8, 9 13, 14, 17 and 18 in view of the cancellation of these claims.

As demonstrated above, Notes 129 and Seiji each fail to disclose or suggest features (1)-(3) of claims 1, 11 and 19.

Similarly, Yamamoto also fails to disclose or suggest features (1)-(3) of claims 1, 11 and 19. Therefore, no obvious combination of Notes 129, Seiji and Yamamoto would result in the subject matter of claims 1, 11 and 19, since Notes 129, Seiji and Yamamoto, either individually or in combination, fail to disclose or suggest each and every feature of claims 1, 11 and 19.

Furthermore, in view of the distinctions discussed above, Applicant respectfully submits that one skilled in the art would not have been motivated or have reason to modify Notes 129, Seiji and Yamamoto in such a manner as to result in, or otherwise render obvious, the subject matter or claims 1, 11 and 19. Accordingly, for at least the foregoing reasons, Applicant respectfully submits that claims 1, 11 and 19, as well as claims 2-4 and 21-26 which depend therefrom, are patentable over the applied references.

II. Conclusion

In view of the foregoing amendments and remarks, it is respectfully submitted that the present application is clearly in condition for allowance. Accordingly, a favorable examination and consideration of the instant application are respectfully requested.

If, after reviewing this Amendment, the Examiner believes there are any issues remaining which must be resolved before the application can be passed to issue, the Examiner is respectfully requested to contact the undersigned by telephone in order to resolve such issues.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: June 23, 2008

By: /Jonathan R. Bowser/
Jonathan R. Bowser
Registration No. 54574

P.O. Box 1404
Alexandria, VA 22313-1404
703 836 6620